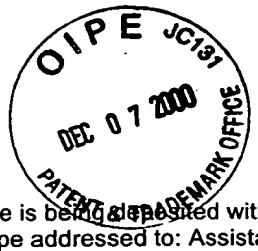
#4



Docket No.: GR 99 P 2348

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

By:_____ Date: November 29, 2000

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Gero Offer
Appl. No.	:	09/621,432
Filed	:	July 21, 2000
Title	:	Method and Apparatus for Authentication for a Multiplicity of Services

CLAIM FOR PRIORITY

Hon. Commissioner of Patents and Trademarks,
Washington, D.C. 20231

Sir:

Claim is hereby made for a right of priority under Title 35, U.S. Code, Section 119, based upon the German Patent Application 199 34 278.4 filed July 21, 1999.

A certified copy of the above-mentioned foreign patent application is being submitted herewith.

Respectfully submitted,

_____
MARKUS NOLFF
REG NO. 37,006

Date: November 29, 2000

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101

/mjb

BUNDESREPUBLIK DEUTSCHLAND

#4

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 199 34 278.4

Anmeldetag: 21. Juli 1999

Anmelder/Inhaber: Siemens Aktiengesellschaft, München/DE

Bezeichnung: Verfahren und Vorrichtung zur Authentifikation für eine Vielzahl von Diensten

IPC: H 04 L, G 06 F, G 07 F

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 3. August 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Weihmayr

CERTIFIED COPY OF PRIORITY DOCUMENT

A 9161
03/00
EDV-L

Beschreibung

Verfahren und Vorrichtung zur Authentifikation für eine Vielzahl von Diensten

Die Erfindung betrifft ein Verfahren zur Authentifikation für eine Vielzahl von Diensten nach Patentanspruch 1 und ein Verfahren zur universellen Authentifikation in einem intelligenten Netz für eine Vielzahl von IN-Diensten nach Patentanspruch 2 sowie eine Vorrichtung zur Authentifikation für eine Vielzahl von Diensten nach Patentanspruch 3.

Viele Personen nutzen heutzutage verschiedenste Dienste, für die sie eine Zugangsberechtigung benötigen. Als Beispiele seien hier nur genannt: Telekommunikationsdienste wie beispielsweise Abfragen einer Datenbank oder Zugang zum Internet, Mobiltelekommunikationsdienste, elektronische Bankdienste. Nahezu jeder dieser Dienste erfordert als Zugangsberechtigung ein Paßwort, eine PIN (Personal Identification Number) oder eine personenspezifische Karte wie beispielsweise eine Kreditkarte, eine Geldautomatenkarte oder Mobiltelefonkarte.

Da Notizen über Paßwörter oder PINs ein Sicherheitsrisiko darstellen, muß sich jede Person die ihr zugeordneten Zugangsberechtigungen merken und Zugangskarten wie Firmenausweise, Bankkarten, etc. sicher verwahren. Gerade zur Verwaltung einer großen Anzahl von Paßwörtern und PINs sind kleine elektronische Datenbanken in Form eines Taschenrechners erhältlich, in denen die Paßwörter und PINs abgespeichert werden können. Die in einer solchen Datenbank abgelegten Informationen sind wiederum durch ein Paßwort oder PIN gesichert, um unberechtigten Zugriff auf diese sicherheitsrelevanten Daten zu verhindern. Der Datenbankbesitzer braucht sich dann nur noch das Paßwort oder die PIN für den Zugriff auf die in der Datenbank gespeicherten Informationen zu merken. Allerdings muß der Datenbankbesitzer beim Zugriff auf einen Dienst zuerst die Zugangsberechtigung für den Dienst

aus seiner Datenbank abfragen und dann manuell in beispielsweise ein Zugangsterminal für den Dienst eintippen. Dies ist weiterhin sehr umständlich und bringt dem Datenbankbesitzer lediglich den Vorteil, daß er sich nicht so viele Zugangsberechtigungen merken muß. Zudem liegen alle Zugangsberechtigungen zusammengefaßt lokal vor, so daß keine Sicherheit gegen Betrug oder Mißbrauch beispielsweise durch Hacker gewährleistet ist.

Die der vorliegenden Erfindung zugrunde liegende Aufgabe liegt daher darin, ein Verfahren und eine entsprechende Vorrichtung vorzuschlagen, die einem Nutzer den Zugang zu einer Vielzahl von Diensten erleichtert.

Diese Aufgabe wird durch ein Verfahren mit den Merkmalen von Patentanspruch 1 oder Patentanspruch 2 und durch eine Vorrichtung mit den Merkmalen von Patentanspruch 3 gelöst.

Die Erfindung betrifft ein Verfahren zur Authentifikation für eine Vielzahl von Diensten, wobei jeder Dienst über eine dienstspezifische und/oder teilnehmerspezifische Zugangsberechtigung aufgerufen wird, ein Authentifikations-Server vorgesehen ist, in dem Authentifikations-Server mindestens eine dienstspezifische bzw. teilnehmerspezifische Zugangsberechtigung für einen Dienst gespeichert ist, eine Vielzahl von Nutzern zugeordneten Authentifikationskodes im Authentifikations-Server gespeichert ist, jeder Authentifikationskode der oder den dienstspezifischen bzw. teilnehmerspezifischen Zugangsberechtigung(en) eines Nutzers zugeordnet ist, und der Authentifikations-Server bei Anforderung eines Dienstes eine Authentifikation mittels eines empfangenen Authentifikationskodes derart durchführt, daß der empfangene Autentifikationskode mit allen im Authentifikations-Server gespeicherten Authentifikationskodes verglichen wird und der zentrale Authentifikations-Server bei einem positiven Vergleichsergebnis eine Verbindung zu dem angeforderten Dienst aufbaut.

Vorteilhafterweise sind bei diesem Verfahren alle Zugangsberechtigungen eines Nutzers für eine Vielzahl von Diensten in einem Authentifikations-Server zentral gespeichert. Der Authentifikations-Server kann dabei Teil eines Telekommunikationsnetzes sein und beispielsweise von einem Nutzer zur Nutzung von besonderen Diensten des Telekommunikationsnetzes über eine dafür vorgesehene Nummer angewählt werden. Sobald zwischen einem Teilnehmerendgerät des Nutzers und dem Authentifikations-Server eine Verbindung besteht, kann der Nutzer beispielsweise durch die Eingabe eines dienstspezifischen Kodes einen der besonderen Dienste des Telekommunikationsnetzes anfordern. Der dienstspezifische Kode kann dazu als Teil einer Rufnummer für einen Verbindungsaufbau zum Authentifikations-Server gebildet sein oder der Authentifikations-Server weist eine "Prompt & Collect"-Funktionalität auf, in der ein dienstspezifischer Kode vom Nutzer übermittelt und daraufhin der Nutzer sich durch Übertragung seines Authentifikationskodes authentifiziert. Der Authentifikationskode entspricht sozusagen einem zentralen Zugangsschlüssel zu den einzelnen Zugangsberechtigungen für Dienste. Der Nutzer benötigt somit nur noch den Authentifikationskode, um Dienste anzufordern. Zur Erhöhung der Sicherheit kann die Übertragung des Authentifikationskodes zum Authentifikations-Server zusätzlich insbesondere zeitlich verschlüsselt werden.

Die Erfindung betrifft ferner ein Verfahren zur Authentifikation in einem intelligenten Netz für eine Vielzahl von IN-Diensten, wobei jeder IN-Dienst über eine dienstspezifische und/oder teilnehmerspezifische Zugangsberechtigung aufgerufen wird, ein Authentifikations-Server in einem Service-Control-Point des intelligenten Netzes vorgesehen ist, in dem Authentifikations-Server mindestens eine dienstspezifische bzw. teilnehmerspezifische Zugangsberechtigung für einen IN-Dienst gespeichert ist, eine Vielzahl von Nutzern zugeordneten Authentifikationskodes im Authentifikations-Server gespeichert ist, jeder Authentifikationskode der oder den dienstspezifischen bzw. teilnehmerspezifische Zugangsberech-

tigungen eines Nutzers zugeordnet ist, und der Authentifikations-Server bei Anforderung eines IN-Dienstes eine Authentifikation mittels eines empfangenen Authentifikationskodes derart durchführt, daß der empfangene Authentifikationskode mit allen im Authentifikations-Server gespeicherten Authentifikationskodes verglichen wird und der Authentifikations-Server bei einem positiven Vergleichsergebnis eine Verbindung zu dem angeforderten IN-Dienst aufbaut.

Weiterhin betrifft die Erfindung eine Vorrichtung zur Authentifikation für eine Vielzahl von Diensten, wobei ein Authentifikations-Server vorgesehen ist, der einen Speicher, in dem mindestens eine dienstspezifische Zugangsberechtigung für einen Dienst und Authentifikationskodes gespeichert sind, eine Vergleichseinrichtung, die einen empfangenen Authentifikationskode mit den im Speicher gespeicherten Authentifikationskodes vergleicht, und eine Verbindungsaufbaueinrichtung zum Aufbau einer Verbindung zu einem angeforderten Dienst aufweist.

Weitere Vorteile und Anwendungsmöglichkeiten der Erfindung ergeben sich aus der nachfolgenden Beschreibung in Verbindung mit der Zeichnung. In der Zeichnung zeigt:

Fig. 1 ein Blockschaltbild, das den Zugriff über verschiedene Zugänge auf verschieden Dienste darstellt,

Fig. 2 ein Blockschaltbild, das den Zugriff über ein elektronisches Zahlungsterminal auf einen Bank-Server darstellt,

Fig. 3 ein Blockschaltbild, das den Zugriff über ein Terminal auf einen Polizeidaten-Server darstellt, und

Fig. 4 ein Blockschaltbild mit dem Aufbau des Authentifikations-Servers.

In Fig. 1 ist der Ausschnitt eines intelligenten Netzes mit einem Service-Switching-Point 1 (SSP) und einem Service-Control-Point 2 (SCP) dargestellt.

Der Service-Switching-Point 1 stellt die Schnittstelle zwischen dem intelligenten Netz und dem öffentlichen Telefonnetz (PSTN: Public Switch Telefone Network) dar. Über eine Vielzahl verschiedener Einrichtungen kann über den Service-Switching-Point auf die verschiedenen Dienste des intelligenten Netzes zugegriffen werden.

Solche Einrichtungen können beispielsweise ein Mobilfunk-Telefon 3 oder ein analoges Telefon 4 und ein digitales Telefon 6, die beide über eine Nebenstellenanlage (PBX: Private Branche Exchange) 5 mit dem Service-Switching-Point 1 verbunden sind, ein Computer mit einem Modem 7, ein Computer mit einem LAN-Anschluß 8 oder ein elektronisches Zahlungsterminal 9 sein. Die vorgenannte Aufzählung ist dabei nicht abschließend, es sind jederzeit weitere Einrichtungen für den Zugriff auf Dienste des intelligenten Netzes denkbar.

Der Service-Switching-Point 1 ist mit einem Service-Control-Point 2 des intelligenten Netzes verbunden. Der Service-Control-Point 2 führt dabei die Dienste des intelligenten Netzes, die sogenannten IN-Dienste, aus. Dazu baut der Service-Control-Point 2 eine Verbindung zu einem Dienst-Server, der einen entsprechenden IN-Dienst ausführt, auf und fordert von diesem den Dienst an.

Als Dienst-Server sind beispielsweise ein Bank-Server 10, ein Universal-Personal-Telecommunication-SCP 11, ein Virtual Private Network 12, ein Home Location Register/Corporate Network 13, ein Data-VPN 14 und ein Kreditkarten-Server 15 vorgesehen, die mit dem Service Control Point 2 verbunden sind.

Mit dem Service-Switching-Point 1 und dem Service-Control-Point 2 ist ferner ein Authentifikations-Server 16 verbunden,

der zur Authentifikation von Zugriffen auf die IN-Dienste vorgesehen ist.

Wird beispielsweise über einen Computer mit Modem 7 eine Verbindung zu einem Bank-Server 10 für z.B. eine Geldtransaktion angefordert, so leitet der Service-Switching-Point 1 die Dienstanforderung an den Authentifikations-Server 16 weiter, der den Zugriff dadurch authentifiziert, daß er einen von dem Computer mit Modem 7 übermittelten Authentifikationskode eines Nutzers mit gespeicherten Authentifikationskodes vergleicht und bei einem positiven Vergleichsergebnis über den Service-Control-Point 2 den IN-Dienst bei dem Bank-Server 10 anfordert. Nach erfolgreicher Authentifikation steht somit eine Verbindung zwischen dem Computer mit Modem 7 und dem Bank-Server 10 zur Verfügung. Analog verläuft beispielsweise ein Zugriff über den Computer mit Modem 7 auf einen IN-Dienst des Kreditkarten-Servers 15. Auch bei der Wahl einer anderen Einrichtung für den Zugang, beispielsweise dem Mobilfunk-Telefon 3, verläuft der Zugang ähnlich. Hierzu überträgt das Mobiltelefon den Authentifikationskode an den Authentifikations-Server 16.

Der Authentifikationskode kann bei einem Zugang über einen Computer per Tastatur von einem Nutzer eingegeben werden oder beispielsweise auf einer SMART-Card hinterlegt sein. Weist eine Zugangseinrichtung beispielsweise einen Fingerabdruck-Sensor auf, so kann der Authentifikationskode als verschlüsselter Fingerabdruck im Authentifikations-Server 16 gespeichert sein, so daß ein Nutzer sich durch seinen Fingerabdruck authentifiziert. Dazu sind im Authentifikations-Server Daten über den Fingerabdruck sowie die zugehörigen Verschlüsselungsinformationen, die zur verschlüsselten Übertragung der Fingerabdruck-Daten dienen, gespeichert.

In Fig. 2 ist skizziert, wie über ein beliebiges Terminal 50, beispielsweise ein Computerterminal, auf einen Bank-Server 52 über einen Authentifikations-Server 51 zugegriffen wird.

Hierzu ist lediglich zu bemerken, daß die Übermittlung des Authentifikationskodes vom Terminal 50 an den Authentifikations-Server 51 mittels einer verschlüsselten Übertragung stattfindet. Dies verhindert unerlaubte Zugriffe auf den Authentifikationskode wie beispielsweise Abhörmaßnahmen auf der Übertragungsstrecke zwischen dem Terminal 50 und dem Authentifikations-Server 51. Für eine zusätzlich erhöhte Sicherheit wechselt der Algorithmus zur Verschlüsselung zeitlich. Diese Anwendung bietet sich beispielsweise zum Transfer von Geldbeträgen auf eine elektronische Geldbörse oder bei der Bezahlung per Kredit- und/oder Accountkarte an.

Ähnlich verläuft der in Fig. 3 dargestellte Zugriff auf die Daten eines Polizeidaten-Servers 102. Einerseits ist der Zugriff ohne Authentifikation mittels eines Polizei-Terminal 103 möglich, auf das ausschließlich dafür autorisierte Personen wie beispielsweise Polizeibeamte Zugriff haben, andererseits kann über ein Terminal 100 und einen Authentifikations-Server 101 ebenfalls auf die Daten des Polizeidaten-Servers 102 zugegriffen werden. Dies erleichtert beispielsweise den Zugriff auf Polizeidaten über ein mobiles Terminal in einem Polizeiauto oder von einer Polizeistreife. Hierbei ist wiederum eine verschlüsselte Übertragung 104 zwischen dem Terminal 100 und dem Authentifikations-Server 101 vorgesehen.

In Fig. 4 ist der Aufbau des Authentifikations-Servers skizziert. Der Authentifikations-Server weist einen Zugangsberechtigungsspeicher 150 auf, in dem eine Vielzahl von Authentifikationskodes gespeichert sind. Für jeden Authentifikationskode ist zudem gespeichert, für welche Dienste ein Nutzer zugelassen ist. Eine Vergleichseinrichtung 151 vergleicht dabei einen übermittelten Authentifikationskode mit allen im Zugangsberechtigungsspeicher 150 abgelegten Authentifikationskodes und signalisiert bei einem positiven Vergleich einer Verbindungsaufbaueinrichtung 152, welcher Dienst angefordert werden soll.

Patentansprüche

1. Verfahren zur Authentifikation für eine Vielzahl von Diensten, wobei

- jeder Dienst (10 - 15; 52; 102) über eine dienstspezifische und/oder teilnehmerspezifische Zugangsberechtigung aufgerufen wird,
- ein Authentifikations-Server (16; 51; 101) vorgesehen ist,
- in dem Authentifikations-Server (16; 51; 101) mindestens eine dienstspezifische bzw. Teilnehmerspezifische Zugangsberechtigung für einen Dienst (10 - 15; 52; 102) gespeichert ist,
- eine Vielzahl von Nutzern zugeordnete Authentifikationskodes im Authentifikations-Server gespeichert ist,
- jeder Authentifikationskode der oder den dienstspezifischen bzw. teilnehmerspezifischen Zugangsberechtigungen eines Nutzers zugeordnet ist, und
- der Authentifikations-Server (16; 51; 101) bei Anforderung eines Dienstes eine Authentifikation mittels eines empfangenen Authentifikationskodes derart durchführt, daß der empfangene Authentifikationskode mit allen im Authentifikations-Server gespeicherten Authentifikationskodes verglichen wird und der Authentifikations-Server (16; 51; 101) bei einem positiven Vergleichsergebnis eine Verbindung zu dem angeforderten Dienst aufbaut.

2. Verfahren zur universellen Authentifikation in einem intelligenten Netz für eine Vielzahl von IN-Diensten, wobei

- jeder IN-Dienst (10 - 15; 52; 102) über eine dienstspezifische und/oder teilnehmerspezifische Zugangsberechtigung aufgerufen wird,

- ein Authentifikations-Server (16; 51; 101) in einem Service-Control-Point des intelligenten Netzes vorgesehen ist,
- in dem Authentifikations-Server (16; 51; 101) mindestens eine dienstspezifische bzw. teilnehmerspezifische Zugangsberechtigung für einen IN-Dienst (10 - 15; 52; 102) gespeichert ist,
- eine Vielzahl von Nutzern zugeordnete Authentifikationskodes im Authentifikations-Server gespeichert ist,
- jeder Authentifikationskode der oder den dienstspezifischen bzw. teilnehmerspezifischen Zugangsberechtigungen eines Nutzers zugeordnet ist,
- der Authentifikations-Server (16; 51; 101) bei Anforderung eines IN-Dienstes eine Authentifikation mittels eines empfangenen Authentifikationskodes derart durchführt, daß der empfangene Authentifikationskode mit allen im Authentifikations-Server gespeicherten Authentifikationskodes verglichen wird und der Authentifikations-Server (16; 51; 101) bei einem positiven Vergleichsergebnis eine Verbindung zu dem angeforderten IN-Dienst aufbaut.

3. Vorrichtung zur Authentifikation für eine Vielzahl von Diensten, wobei
ein Authentifikations-Server (16; 51; 101) vorgesehen ist, der

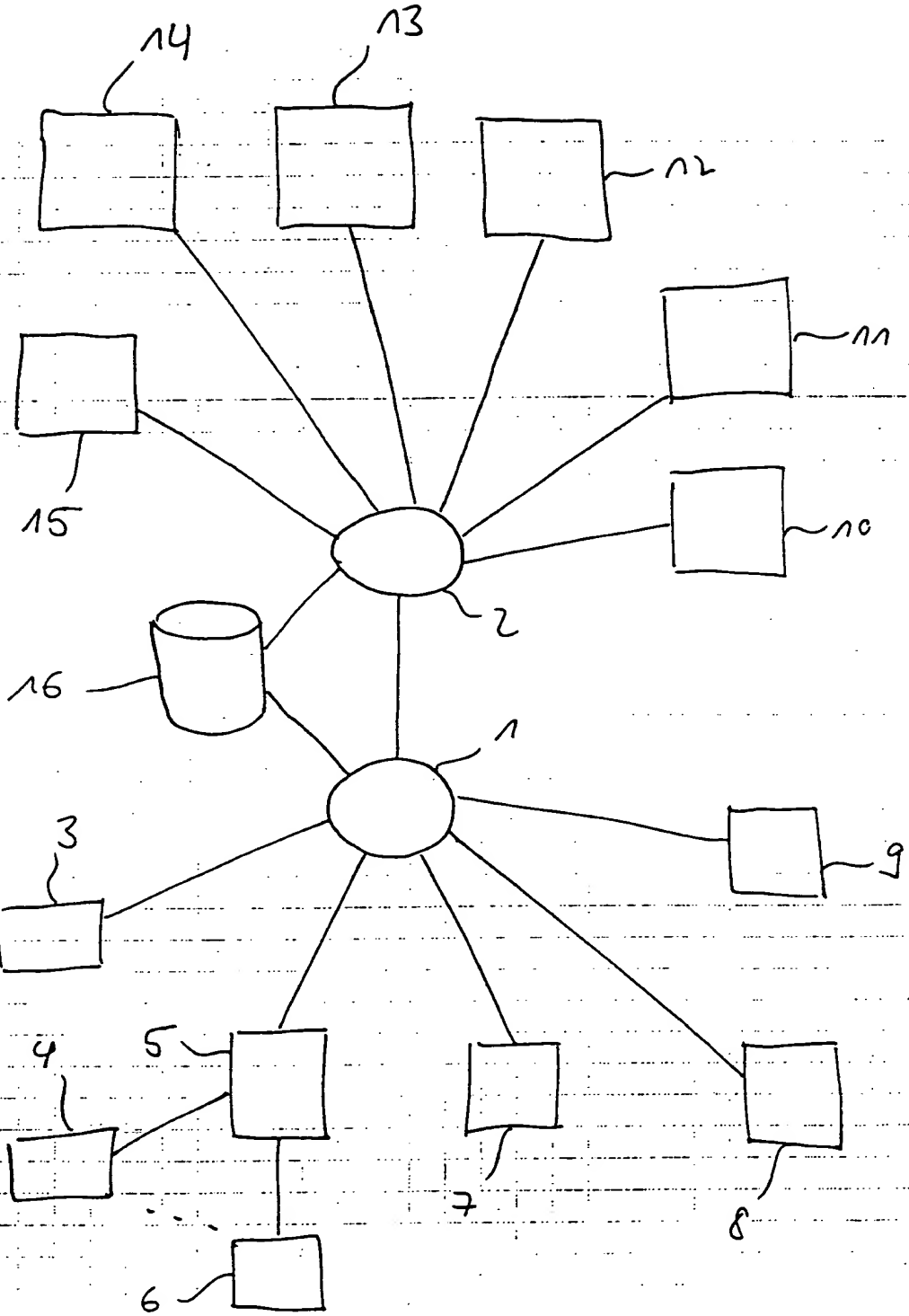
- einen Speicher (150), in dem mindestens eine dienstspezifische Zugangsberechtigung für einen Dienst (10 - 15; 52; 102) und Authentifikationskodes gespeichert sind,
- eine Vergleichseinrichtung (151), die einen empfangenen Authentifikationskode mit den im Speicher (150) gespeicherten Authentifikationskodes vergleicht, und
- eine Verbindungsaufbaueinrichtung (152) zum Aufbau einer Verbindung zu einen angeforderten Dienst aufweist.

Zusammenfassung

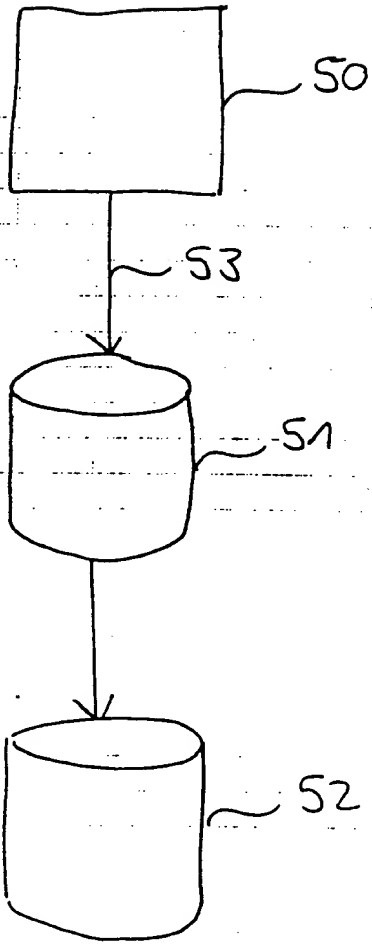
Verfahren und Vorrichtung zur Authentifikation für eine Vielzahl von Diensten

Die Erfindung betrifft ein Verfahren zur Authentifikation für eine Vielzahl von Diensten, wobei jeder Dienst über eine dienstspezifische und/oder teilnehmerspezifische Zugangsberechtigung aufgerufen wird. Ferner betrifft die Erfindung ein Verfahren zur Authentifikation in einem intelligenten Netz für eine Vielzahl von IN-Diensten. Weiterhin betrifft die Erfindung eine Vorrichtung zur Authentifikation für eine Vielzahl von Diensten.

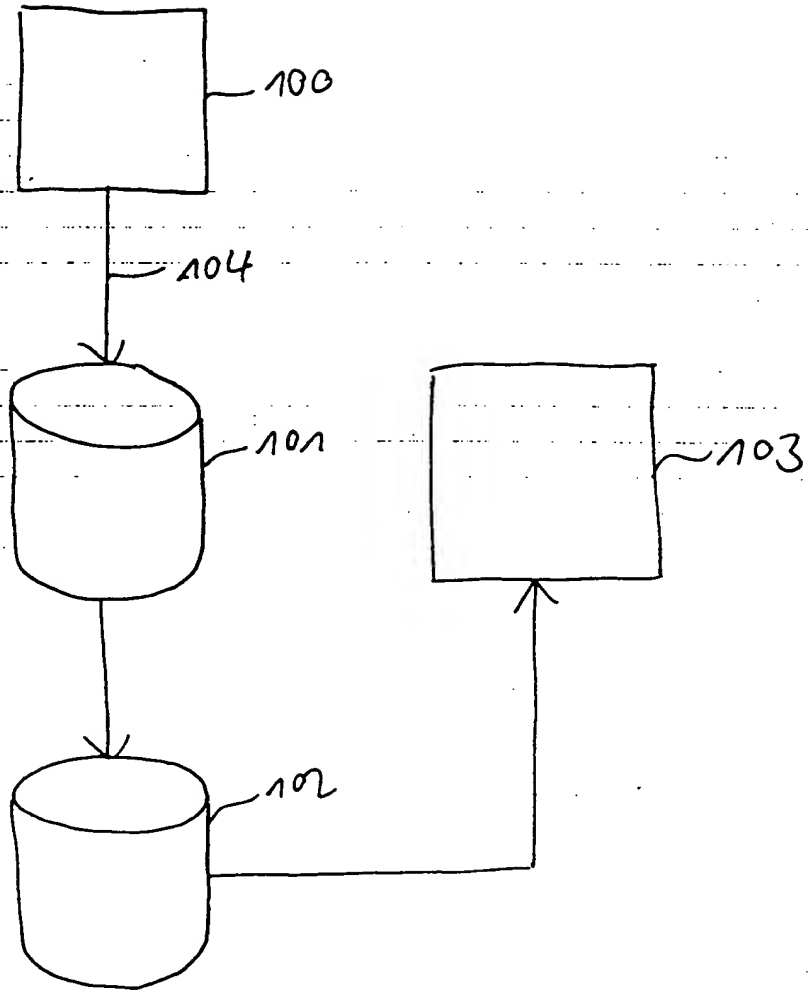
(Fig. 1)



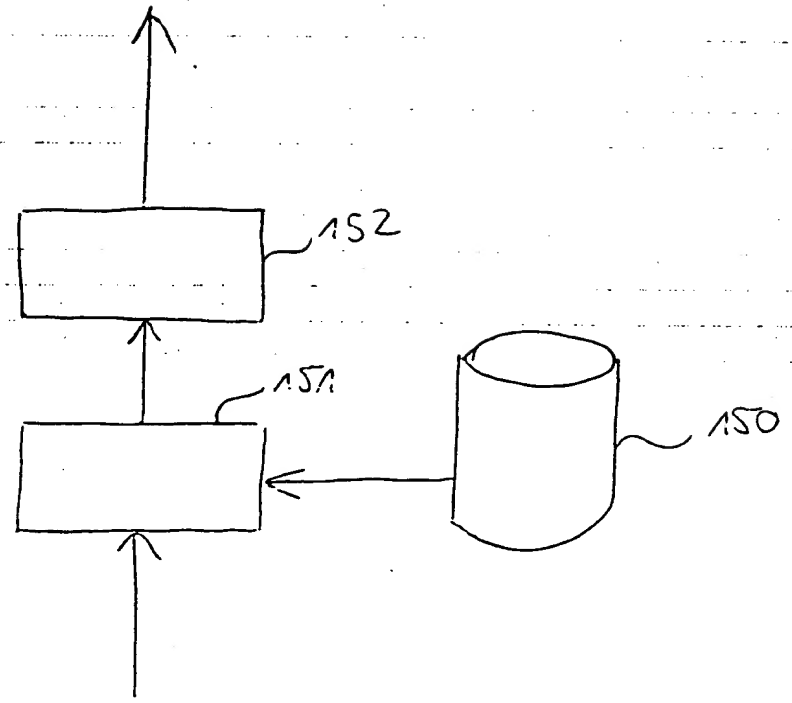
Figur 1



Figur 2



Figur 3



Figur 4